QUALYS

All you need to know about the FREAK vulnerability

Researchers have identified that a MITM attack can potentially force HTTPS connections to use weaker and easier to crack encryption.

HADI JAAFARAWI,
MANAGING DIRECTOR, QUALYS ME

"Most organizations don't realize that it's their own actions that are proving to be bigger problems in practice.It is therefore important for businesses in the Middle East to ensure that systems and software are updated to avoid any potential threats."

This past year we have seen an overwhelming interest in FREAK or "Factoring RSA EXPORT Keys."FREAK is a vulnerability in Secure Socket Layer (SSL) that allows an attacker that has a Man-in-the-Middle (MITM) position to downgrade your computer's SSL communication to an export grade cipher, which can easily be broken and accessed in less than 24 hours. Once the attacker has the key they can eavesdrop or modify your communication, and redirect you to impostor sites.While the full impact of this vulnerability is yet to be known, we do know that browsers, web clients and hosts can negotiate the strongest encryption "allowed," falling back to weaker, "export" protocols as required.

How It Works

Researchers have identified that a MITM attack can potentially force HTTPS connections to use weaker and easier to crack encryption. This vulnerability affects clients that communicate with servers that offer RSA_EXPORT cipher suites and are using a implementation of SSL that is vulnerable to FREAK, which includes Microsoft Windows's Secure Channel (SChannel), Apple's and Android's OpenSSL based libraries. The server part itself is not vulnerable, but a server can avoid its client from being attacked by not offering the RSA_EXPORT ciphers.

An attacker connects to the web server with an export cipher and gets a message signed with the weak RSA key. Key gets cracked. For any future connections from innocent browsers, the attacker can act as a man in the middle (MiTM) connecting to clients, who will accept it. The attacker will then have access to all communication between the client and server.If hackers are successful, they could spy on communications as well as infect PCs with malicious software.

As processing power increases and reduces the time and cost of breaking encryption, there is a direct impact to the security of weaker, shorter keys. While an RSA 512-bit key a few decades ago might have been considered a good option, it is not so today. The first 512-bit key was broken in 1999 and currently can be done through the use of on-demand computing power cloud provider in around seven hours at a low cost.

What You Can Do

Since the detection of the vulnerability was announced in March of this year, Apple, Google and Microsoft have released security patches to fix this problem. However these types of vulnerabilities are a reminder of the importance of good security hygiene within our networks and communication infrastructure. There has never been so much scrutiny of the security of the Secure Socket Layer (SSL) and Transport Security Layer (TLS) protocols like today. But, although most attention is on the protocol vulnerabilities, most organizations don't realize that it's their own actions that are proving to be bigger problems in practice.It is therefore important for businesses in the Middle East to ensure that systems and software are updated to avoid any potential threats.

As cyberattacks continue to become more advanced, organizations are being forced to adapt to address new threats. In this complex security landscape, it is critical to be proactive and vigilant to protect against cyber threats in order to be as secure as possible. Practicing good cyber hygiene is the cornerstone to achieving this and in the enterprise, this includes:

- Ensuring that only authorized devices are connected to company networks that limits the applications or software running on a company's assets to only those necessary to meet business needs.
- Securely configuring corporate assets, removing default usernames and passwords and restricting the use of administrative privileges.
- Continuously scanning for vulnerabilities and misconfigurations in company assets, and deploying a combination of network and endpoint malware defences using a mix of technologies, including blacklisting, whitelisting, heuristics, and virtualization.

Qualys' SSL Labs offers a free SSL Server Test that will tell users if their website's server supports "export-grade" cipher suites, which are at the root of the vulnerability. Enter a domain name of any website into the SSL Server Test's field, then examine the resulting report.